THE COMPREHENSIVE LEGAL INSIGHT ON THE PROTECTION OF THE WOMEN WORKING IN EDUCATION SECTOR FROM THE GENDER BASED CYBER CRIME: AN INDIAN PERSPECTIVE

A

SYNOPSIS

(THESIS PROPOSAL)

SUBMITTED TO

THE ICFAI UNIVERSITY, DEHRADUN

IN PARTIAL FULFILLMENT OF THE REQUIREMENT

FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY (Ph.D.)

IN

Law

BY

Rupaksh Sharma

(Enrollment No: RSILS180080)

Under the Supervision of

Dr. Susanta Kumar Shadangi

ICFAI law School

The ICFAI University, Dehradun

2023

R Sharma

Candidate's Declaration

I, **Rupaksh Sharma,** declare that the synopsis entitled, **"The comprehensive legal insight on the protection of the women working in education sector from the gender based cybercrime: An Indian Perspective"** being submitted in the partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in Law under ICFAI law School, The ICFAI University, Dehradun during the academic year 2022-23.

It is the work that is expected to carry out under the supervision of Dr. Susanta Kumar Shadangi. It is further declared that the synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

Signature R Sharma **Date:** 31.01.2023

Candidate's Name Rupaksh Sharma

The ICFAI University, Dehradun

CERTIFICATE

This is to certify that the thesis entitled, "**The comprehensive legal insight on the protection of the women working in education sector from the gender based cybercrime : An Indian Perspective"** is an original piece of work done by ***Rupaksh Sharma*** under my supervision being submitted in the partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in Law under ICFAI Law School, The ICFAI University, Dehradun during the academic year 2022-23.

Further, It is certified that the synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

Susanta Kumar Shadangi

Signature of the Supervisor in full

Name in Capital Letters SUSANTA KUMAR SHADANGI

Designation & Address Associate Professor,
ICFAI Law School.
ICFAI University, Dehradun.

TABLE OF CONTENT

	Page No
Abstract	i
Introduction	1-2
Research problem	03
Literature review	4-11
Research objectives	11
Methodology of research study	11
Expected outcome of the result	13
Hypothesis	13
Tentative Chapterisation	14-15
Month wise plan of work	15
Bibliography	16-17
Plagiarism Report	18

ABSTRACT

We are living in the Era of cyberspace and technology. We are dependent on the internet for the various purposes of the day to day life. The scope of the internet is not only limited to completing the various tasks of life but it's been a medium of communication and expression. Recently, the need for the internet increased during the Covid 19 pandemic, where using the same was the only option left with all of us. Cyberspace comes up with the scope of connecting life with various areas but it has contained flaws too. If not recognized and acknowledged by law and society it may increase the violations of various rights related to Cyberspace. Specifically, the venerable group of society will be suffered the most. The vulnerability related to cyberspace increases when the legal system of the state is not efficient and does not recognize undiscovered and new forms of crime in society. Vulnerability on the basis of gender and age is most common in the case of cybercrime. Women and children are mostly suffering from cybercrime as they are easy to be targeted. Children due to their immature age suffer from crimes like cyber pornography, stalking, and another form of crime. On the contrary, women suffer cause of their gender and are unable to recognize the kind of crime due to unawareness in society. The internet hides a number of crimes within it. It includes crime-related women the most. The Indian legal system provides protection against cyber-crime under the Information technology act of, 2000 but its lacks in identifying and developing crimes related to cyber law.

The information technology act 2000 provides several laws which authenticate e-commerce, E-signature, and protection against crime related to cyberspace. The IT act 2000 was further amended in the year 2008 to fulfill the need of society. The criminal amendments 2013 introduced the changes into the criminal laws. It changed provisions related to the Indian penal code where the crime against women was introduced in a more advanced form and included under it the provisions related to the cybercrime.

INTRODUCTION

"The online abuse and trolling of women in India should be treated the same way as violence in real world"[1]

Smt. Maneka Gandhi

Former Union Minister, Women and child Development

Information and communication Technology (ICT) and the internet are an essential part of the present scenario. The requirement of the internet is highly prominent that one cannot imagine their basic need to be completed without using it. The dependency of the people on the internet grew especially during Covid -19 pandemic, not only the adults but also children were wholly reliant on the internet for fulfilling their basic needs, for example right to education. ICT and cyberspace provided people various rights using online tools like using social media, performing work responsibility from home and providing social, political and economic rights.

Despite of growth of the internet user in India there are inequalities among the users. For example, the number of internet users, the number of Facebook and Twitter users, the level of digital literacy, and political tweets all show this trend. According to a research by Boston Consulting Group and the Retailers Association of India, women account up 29 percent of India's internet users. The remaining 71 percent are men. One of the primary factors that contribute to this phenomenon is the unequal access to the internet that is experienced by men and women.[2]

Technical abuse can be seen more against women. Gender based violence under cyberspace is very common in India. The prediction states that women are the most vulnerable target for the perpetrator of cybercrime. The existing social norms make women soft targets. The long rooted social norms of patriarchy make them responsible to hold the reputation of their own as well as the Family members. Very few cases are registered against these cybercrimes. The reasons for not filing the cases can be many including lack of specific defining laws, Non applicability of the law on the extra territorial subject matter especially between India and the foreign country which are host of interest. According to the report of National Crime bureau 2013, for the very first time, published the number of cases against women was registered. One of the major reasons for

---

1 Cyber Violence against Women in India – A Research Report, Japleen Pasricha

2 Rashid Manzoor Bhat, Peer Amir Ahmad , Social Media and the Cyber Crimes Against Women-A Study , Journal of Image Processing and Intelligent Remote Sensing ISSN 2815-0953 Vol: 02, No. 01, Dec 2021–Jan 2022

less reporting of the cases is unawareness about the violation of their rights by the victim, the common people as well as officer in charge or authorities. In the year of 2001 the case of Ritu Kohli became the first reported cybercrime case in India[3]

In the case of Ritu Kohli **(MANISH KATHURIA VS RITU KOHLI)**[4] the petitioner was being stalked by the defendant for four consecutive days. The defendant was chatting illegally by using her name and using obnoxious and obscene words. He also distributed her contact number and invited them to chat. Due to this, she started getting many calls in odd hours. Because of this she went in a state of shock and finally reported the case to Delhi Police. The accused was booked under sec 509 of IPC for Insulting the modesty of women. Thus sexual abuse that took place on the street or in physical form can be reported immediately but online gender abuse needed to be handling by the victim herself.

Justice Prabha pointed out that the **law and its officers continue to operate in the dimension of the physical only, and are consequently always searching for physical signs of injury, despite the consequences of gender-based cyber violence (GBCV) being as debilitating as crimes offline. Seeking to optimize its limited resources, law enforcement agencies would rather expend their time and energy in what they perceive to be crimes with 'real' harm like rape and murder.**[5]

The main reason for unawareness about the cybercrime is weak cyber legislation as The Information Technology Act, 2000 does not provide the effective defense legal remedies to most of the cybercrime.

---

[3] NILESH BELIRAYA K AND ABHILASHA , Cyber Crime against Women in India: Legal Challenges and Solutions, International journal of law management & humanities [ISSN 2581-5369]

[4] Manish Kathuria Vs Ritu Kohli, C.C. No. 14616/2014

[5] Justice Prabha Sridevan (retd.), Madras High Court, Chennai, report of the national dialogue on gender-based cyber violence, organized by it for change, Bengaluru & advanced Centre for women's studies, TISS, Mumbai

RESEARCH QUESTIONS-

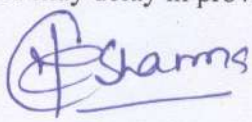
1. What are the lacunas under Indian Legislations related to protection of working women in education sector against cyber-crime?
2. How the involvement of third party or indirect electronic harassment is infringing the right to privacy of working women in India.
3. Whether the foreign nations are incorporating specific and comprehensive Laws regarding cybercrime against women are more efficacious in preventing it.
4. What are remedies available against the issues related to cybercrime committed cross broader and in conflict related to territorial jurisdiction, to prosecute and convict suspect?

Research Problem

There are reasons for Cyber abuse or violence against women in India, but majorly it covers the following-

1. Women are vulnerable and easy target for the abuser of the gender based cyber violence as women generally avoid filing and reporting the cyber-crime due to social and family reputation.
2. Indian legal systems do not provide an effective and comprehensive legal framework for cyber-crime against women.
3. Due to uncertainty of cyberspace and ineffective roles played by the service providers, its challenging to identify the unanimous perpetrators.
4. Territorial and Extra territorial jurisdiction of the State is a great concern in the cases where offences committed cross broader.

Lack of awareness and training among the police officer, service providers and third party can increase the complexity of the cases and may delay in providing justice.



Literature Review

1. **Cybercrime against women and children", Aditi Shrivastara, 2021**[6]

In this article the author provided that with increasing the rare of internet uses, the rate of cybercrime Increased incredibly during the lockdown in India. A total of 704 cybercrimes registered against women in 2020 and 504 in 2021 (till July). Cyber stalking. Sextortion. Cyber-hacking, cyber-Bullying. Sexual Abase including the use of pornographic and sexually explicit material against the victim, Cybersex Trafficking, and Phishing are the most frequent cybercrimes performed against women during the Pandemic. Cyber bulling, child grooming, cybersex trafficking, and sexual abuse of minors are among The most prevalent cybercrime performed against children during the pandemic. Due to their vulnerability women and children were particularly easy prey for cyber criminals and sexual predators during the lockdown.

2. **Cyber Crime and the Victimization of Women: Laws, Rights and Regulations",**[7]

Cyber Crime and the Victimization of Women: A distinctive and significant addition to the literature examining several facets of cybercrime is Laws, Rights and Regulations. This book deals directly with a Topic that is typically only mentioned incidentally, i.e. as a side effect of a particular cybercrime instance or concern. It investigates the gendered aspects of online crimes such cyber bullying, cyber stalking, Defamation modified pornographic photos, and electronic blackmail. Perpetrators who, for a variety of reasons, are unlikely to be identified or punished routinely use these and others methods to intimidate control, and cause other harm, Researchers, academics, legislators, everyday women, and those support them will learn more about cyber victimization and how to better respond to cybercrimes

3. **Law's Expressive Value in Combating Cyber Gender Harassment- Danielle Keats Citron**[8]

In this article author emphasized on the online sexual harassment of women which remain overlooked and trivialized. The harassment affects women's life in many aspects, especially their participation in online life. It undermines their dignity, identity, critiquing the trivialization of

---

[6] Cybercrime regulation & Security: Contemporary ISSUES and Challenges

[7] Debarati Halder, 2011

[8] Danielle Keats Citron, Michigan Law review, vol. 108, issue 3

Sharma

cyber gender harassment. The author describes the situation of the women as she cannot escape from the harassment of the third party and their attack. The author Considered counter speech as a temporary solution against harassment. Further it was stated by the author that the trivialization of cyber gender harassment has unfortunate consequences of under enforcement of criminal laws. The absence of training in the prevention of cyber harassment against women is the reason for the ignorance for filing the criminal cases against perpetrators. **Therefore there is a need for Cyber civil rights laws and agenda to secure the Purpose.**

4. **An Outline On Increasing Online Gender Violence Against Women In India And The Role Of Cyber Security - Adv. Ranjita Madiwale1 , Dr.Sona Kumar[9]**

   The author has shared the views over the increasing cases of online gender violence against Indian women after digital resolution, the article included reports submitted by the NCRB and NCW mentioning the same issue. Analyzing the current internet user in India and women user participation on the Internet, author suggested framing of stronger legislative framework and requirement of joint efforts of the judiciary and government to eliminate this violence.

   Highlighting the legislative gaps, the author stated about the implementation of the Information technology Act, 2000 effectively by the enforcement officers as they are not trained to handle the technologies of investigation of online crime. The role of the third party or fourth party vendors was highlighted as an imperative which cannot be overlooked. The third party can be utilized as a data provider and data receiver in the case of cybercrime against women.

5. **International human rights protection against online gender based violence during the pandemic- aurora fatimatuz zahra[10]**

   The author highlighted on increasing of crime in numbers during Covid -19 pandemic like online sexual harassment. Its most often gender based violence (OGBV) and directed towards women. OGBV is a part of definition of "discrimination against women" provided by CEDAW. As technology facilitated gender based violence against women is included under the ambit of the definition "discrimination against women. Its includes its various elements and impacts on women's life. Further, Author refers to international

[9] Journal of Positive School Psychology, 2022, Vol. 6, No. 6, 3920-3927

[10] Faculty of Law Universities Muhammadiyah Yogyakarta

Sharma

instruments like Universal declaration of Human Rights 1948 and European Union which includes special protection of women against cyber-crime. Ultimately it included methods and protections from OGBV included in the various international Conventions like CEDAW 1979 and UDHR 1948.

6. **Strategies to prevent and control cybercrime against women and girls- s. Poulpunitha, k. Manimekalai, p. Veeramani**

In India, Women are mostly victims of technological fancies. There is minimal proper training and education regarding such developments and ignorance towards this advancement has paved way for cybercrime. Even the officer and authorities has no proper training who handle these cases and essential expertise for undertaking cybercrime against women.

The authors in the major finding of their research concluded on problem and issues of cybercrime against women and girls in order to exhibit the preventive strategies and means to fight back with the support of coercive forces.[11]

7. **Digital abuse of crime against women in India -DR.I. CHITRA** [12]

The article examines women's fear for the digital world. The author stated that the objectives of Information Technology Act, 2000 can be clearly understood by its preamble that it was framed largely for improving E-commerce, therefore its only covers crime relating to economics or commerce, but it did not cover the areas relating to the net users. The crime including the cyber defamation, email spoofing, and cybersex, hacking and trespassing into once privacy nowadays but IT Act is not expressly mention them under any provisions. Whereas the legislations like Indian penal code, constitution of India provides special protection from these offences. In the conclusion, author emphasized on the sociological reasons of not reporting about the cybercrime due to hesitancy and shyness of the victim.

8. **Outlawing cyber-crimes against women in India -Ms. Saumya uma**[13]

The paper outlined the most prevalent types of cybercrime committed against women, covered the substance of each category of offences, examined how the law applied, and highlighted

[11] International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-3, January 2020

[12] SYNDICATE – The Journal of Management Volume 20, March 2020, ISSN 2278-8247

[13] Assistant Professor, Maharashtra National Law University (MNLU), Mumbai.

Sharma

relevant reports, cases, and rulings as examples.

The author went on to say that because neither the IPC's nor the Information Technology Act 2000's provisions adequately reflect the actual experiences of women, the first step in providing legal recourse for women is to ensure that the harassment, intimidation, and violence that women experience online is properly incorporated into written laws through amendments.

In the end, the article examined the reality on the ground and the efficacy of Indian laws in defending women's online rights.

9. **Cyber sexual assault against women- Vulnerability and remedies- Rani Bindu and Gurcharan Singh**[14]

   In this article, several facets of online sexual assault against women have been examined in relation to their susceptibility and subsequent solutions. The authors claimed that new types of crimes against women and girls are emerging. The prevalence of digital technology and their use in communication has led to a greater understanding of gender violence online. Technology has also made it easier for crime against women to occur on various platforms and using a variety of tools. Without taking into account the responsibility and culpability of intermediaries and perpetrators, these crimes are frequently committed across different jurisdictions.

10. **Identification And Mitigation Of Cyber Crimes Against Women In India- Deepak Kumar Verma ,Vinodini Verma, Anamika Pal , Drishti Verma**[15]

    In this Article Author stated that in the current era of digitization, the internet has created a challenging issue for females in relation to cyber security. Girls and women must deal with problems like privacy invasion brought on by emails, e-chats, hate speech, online grooming, spoofing, sexual misconduct, bullying, hacking, cyber stalking, transmitting morphing, obscene materials, and sexual defamation, as well as blackmailing, misrepresenting information for financial gain, or espionage. Women who lack basic computer and internet literacy are a particular target of victimization. Instead of being a tool for communication, online abuse is infamous for being a kind of abuse or violence towards women and girls. In the information technology industry, privacy violations,

[14] 9 Indian Police Journal, Volume 68, Number 4, ISSN 0537 -2429, October-December 2021

[15] International Journal of Advanced Research in Computer and Communication Engineering Impact Factor Vol. 11, Issue 4, April 2022 DOI: 10.17148/IJARCCE.2022.11440

Sharma

unauthorized surveillance, cyber stalking, unauthorized data access, and retribution are all evolving at an increasingly high level.

11. **Social Media and the Cyber Crimes Against Women-A Study- Rashid Manzoor Bhat, Peer Amir Ahmad**[16]

In this article authors started that Indian internet user has been grown in the recent past years and social media has become the part of the life of the Indian user. The user grown in the 67 million in 2022 due to the easy access and availability of Internet, out of the total user women hold 29 percent and whereas 71 percent are male user out of the total user. The author highlighted the participation of women user on social media related to the subjects which are sensitive are very less , which shows the reality of Indian women are exclude from the political process that take place in India. Further it was highlighted that many women internet user deleted or cancelled their accounts owning to the abuse and harassment that women face online.

Additionally, author focused on the social media stalking and its effects on women's life as it need not to be sexual in the nature always rather it can bother and threating the person who has been stalked and violated the privacy of the victim. When this offence is completed on an online platform it's called cyber stalking.

In the end, it was concluded with the suggestions of the preventive measures like ,bullying and harassment that took place against women because of their gender need to be addressed', women feel more secure online if there is a dedicated mechanism in the place conduct warning, suspension and depart forming should be issued to those who engaged in gender based harassment.

12. **Cyber stalking is a social evil: from the Indian women's perspective - Ameema Miftha, Marc Conrad and Marcia Gibson**[17]

In this article authors stated that in India, the prevalent social and cultural value system and conventions may make it difficult for women to contact the police or file legal complaints. The few studies to-date in the Indian context, indicate the high prevalence and serious impacts cyber stalking has on the victims' psychological and physical state.

[16] Journal of Image Processing and Intelligent Remote Sensing ISSN 2815-0953 Vol: 02, No. 01, Dec 2021–Jan 2022

[17] Institute for Research in Applicable Computing The University of Bedfordshire, University Square, Luton, Bedfordshire, UK

Sharma

Additionally, it was discussed how friends' and family members' deeds could cause secondary victimizations. According to the author, this is a sort of social punishment brought on by gender-specific attitudes and beliefs that appear to be prevalent in India. These secondary victimizations were described as having far-reaching, long-term effects that increased the already high levels of distress that are normally felt during cyber stalking situations.

13. **Cyber Stalking Victimization of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspective- DebaRati HalDeR**[18]

The article makes the argument that because restorative justice (RJ) and therapeutic jurisprudence (TJ) are both victim-oriented, the problem of women being stalked online may be handled by RJ, and laws in this area must be examined by legal actors with experience in both RJ and TJ philosophy. India had previously adopted a therapeutic punishment policy to uphold the accused's rights. However, the RJ backdrop in situations of cyber stalking still does not take into account contemporary TJ concepts. Therefore, this article investigates whether retributive principles can be replaced by RJ and TJ principles in cases of cyber stalking victimization. The effectiveness of the Indian cyber stalking statute for victims is also examined from the perspectives of RJ and TJ.

14. **An Analytical Study Relating to the Legal Dimensions against Cyber violence in India (Special Reference in retaliation to porn and blackmailing on the Internet) Ms. Deepali Rani Sahoo1, Dr. Pooja Kapoor**[19]

The authors provided in this article that cyber violence against women includes retaliation of porn and taking revenge by blackmailing on internet. It also gives special reference to the cybercrime relating to pornography and blackmailing through internet. The study of area has been taken in to consideration of certain cases from Delhi NCR region for the proper study.

15. **Gendered discourse: Technology mediated violence and women students- Dr. B. Radha**[20]

---

[18] TEMIDA December 2015, str. 103-130 ISSN: 1450-6637 DOI: 10.2298/TEM1504103H

[19] Asian Journal of Social Science and Management Technology ISSN: 2313-7410 Volume 4, Issue 3, May-June, 2022

[20] Assistant Professor, Department of Communication, Manonmaniam Sundaranar University, Tirunelvel

Sharma

The authors noted that student access to technology-enabled communication devices is increasing day by day. Other than entertainment, these gadgets are mainly used for communication purposes. It's important to understand how these devices have negotiated with traditional gender platforms to create new ones or overcome the old. Specifically, when it comes to abuse, behavioral surveillance, harassment, and stalking, female students are experienced on a gender basis. In addition, the study identified links between the nature of prevalent violence and social patriarchal norms in societies that intersect dimensions such as class, caste, language and religion. It also provided the different intervention strategies used by these female students to address issues across or within gender frameworks.

RESEARCH OBJECTIVES-

1. To Determine responses to cybercrime and security against working women in the education sector by Indian legislation and judiciary
2. To ascertain the combating capacity of the third party against the privacy infringement and data protection of working women.
3. To compare laws existing in the various countries in related to cybercrime against women.
4. To Examine various issues & challenges relating to cybercrime and security against working women in the education sector in India.

METHODOLOGY OF RESEARCH STUDY

The researcher will adopt both doctrinal and empirical research methods to complete the research. To conclude the research under **Empirical method, primary data** will be collected by conducting the survey using questionnaire format, which will be represented by chart, table and graphs.

The study will include **the doctrinal research** with reference to existing legislation, judicial precedent, research articles and law reports. Reports provided by the central crime bureau, National commission for women, National Human Rights commission will be given preference.

Survey location – Dehradun and Roorkee Uttarakhand

Sampling Technique- Convenience sampling and stratified sampling

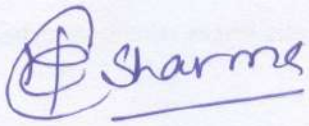
HYPOTHESIS –

1. Existing laws are insufficient to provide protection and security from gender based cybercrime against working women in education sector.
2. Privacy laws are incomplete and weaker to provide security in cyber space against working women.
3. The notion of explicit codified legislation for the protection of the women from online gender-based harassment will not only give recognition to the new forms of cyber-crime against women but also impart it into the legal system effectively.

EXPECTED OUTCOME OF THE STUDY

The present study focuses not only on understanding the idea of cyber-crime but also explains the reasons for the emergence of these crimes at both National and international level. The study includes the analysis of present legislative framework for protection against cyber-crime against women. The study also comprises the new form of developing cyber-crimes and set new standard for controlling the cyber-attacks. The way to overcome these crimes can be done through comprehensive cyber laws, education and policy making, technical training and awareness.

Further study contains the prosecution of the offenders under national and international jurisdiction



TENTATIVE CHAPTERISATION –

TENTATIVE CHAPTERISATION –

Chapter I Introduction –

The chapter will embrace the meaning and concept of Cyber laws. The evolution of the information & communication technology (ICT) will be conferred. The evolution and historical development of the cyber scape and laws will thoroughly be discussed.

Chapter II Conception framework Of Cybercrime against women

This chapter will majorly cover the understanding about Gender based online crime covering the aspects of women's rights. It will include the Meaning, scope and various evolving forms of cyber-crime against women like Cyber stalking, revenge porn, Email spoofing, third party involvement/indirect electronic harassment and trolling and cyber bulling. Furthermore, the chapter will include the impact of these cybercrime as women victimization on their socio- economic and civil life.

Chapter III International Cyber law regime on Women's perspective-

The international legal regime to cybercrimes and global cybercrime picture will be included in this chapter. The comparative analysis of the various legal system regarding the cyber laws and protection provided to women from the gender based cyber-crime will be discussed thoroughly.

Chapter IV **Legislative approach and efficacy to produce remedies for cybercrime against women in India**

The Chapter will analysis the Indian legislative approach towards cybercrime against women including the constitutional perspective like freedom of speech and expression, Information technology act, 2000, Information technology amendment Act, 2009, criminal laws and various issues relating to investigation and use of investigation measures. The chapter will mainly focus on the inefficacy and flows in the IT laws and privacy infringement.

Chapter V Empirical Research-

The chapter will be dedicated to the Empirical Study with reference to the protection of the working women from the gender based cyber-crime or online gender based sexual abuse.

Chapter VI Liability of service provides, investigation officer and judiciary-

The last chapter will emphasis the liability of the services provides, investigation officer and judiciary to combating the Crime against women. It will also include the rights of the women to be forgotten from the cyber crime as it can destroy her modesty, morality and dignity. Further the role of police to register the cyber crime cases correctly according to the crime's nature and its effect on the further investigation will be discussed. Lastly the role of judiciary in combating cyber-crime especially in the territorial and extra territorial jurisdiction will be analysis.

Chapter VII Conclusion and Suggestion –

Sharma

Based on the findings the chapter will highlight some of the current legislation's flows in dealing with the gender based cyber-crime in India and further provide the solution for the dealing with the same effectively.

Bibliography

1. BOOKS-

I. Debarati Halder & K Jaishankar ,Cyber crime against women in India, SAGE Publications Pvt. Ltd; First edition (30 April 2021)

II. Dr. Talat Fatima ,Cyber Crimes, , Eastern Book Company,2018

III. Debarati Halder & K Jaishankar ,Cyber Crime and the Victimization of Women: Laws, Rights and Regulations , Information Science Reference ,2011

2) ARTICLES-

I. Danielle Keats Citron ,Law's Expressive Value in Combating Cyber Gender Harassment, Michigan Law review, vol. 108, issue 3

II. Adv. Ranjita Madiwale1 , Dr.Sona Kumar, An Outline On Increasing Online Gender Violence Against Women In India And The Role Of Cyber Security , Journal of Positive School Psychology, 2022, Vol. 6, No. 6, 3920-3927

III. Aurora fatimatuz Zahra, International human rights protection against online gender based violence during the pandemic, Faculty of Law Universities Muhammadiyah Yogyakarta

IV. S. Poulpunitha, k. Manimekalai, p. Veeramani, Strategies to prevent and control of cybercrime against women and girls , International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-3, January 2020

V. DR.I.CHITRA , Digital abuse of crime against women in India, SYNDICATE – The Journal of Management Volume 20, March 2020, ISSN 2278-8247

VI. Ms. Saumya uma , Outlawing cyber-crimes against women in India , Assistant Professor, Maharashtra National Law University (MNLU), Mumbai

VII. Rani Bindu and Gurcharan Singh,Cyber sexual assault against women- Vulnerability and remedies , 9 Indian Police Journal, Volume 68, Number 4, ISSN 0537 -2429, October-December 2021

VIII. **3) LEGISLATIONS-**

I. The Information Technology Act, 2000
II. The Indian Penal Code, 1860.
III. The Information Technology amendment Act, 2008
IV. The Criminal Law (Amendment) Act, 2013

4) CASES LAWS -

I. Manish Kathuria Vs Ritu Kohli, C.C. No. 14616/2014
II. Suhas katti vs state of Tamil Nadu,C.NO. 4680 of 2004
III. Dr.L.Prakash vs superintendent, Puzhal Central Prison-1, Puzhal, Chennai, laws (MAD)-2008-7-353

Sharma

Month-wise plan of work and targets to be achieved

S. No.	ACTIVITIES	MONTHS															
		J-23		F-23	M-22	--	--	--	--	--	--	--	--	--	--	--	D-22
1	Literature review for identifying the items for Research about the subject				March 23												
2	Exploratory research for studying e-government initiatives taken by Uttarakhand Government																
3	Questionnaire designing	Jan 22															
4	Pilot testing and refinement of questionnaire	Dec 22-jan 23															
5	Data collection	Jan 23															
6	Data collection	Jan 23															
7	Data collection	Jan 23															
8	Data collection			Feb 23													
9	Data preparation			Feb 23													

Sharma

10	Data analysis																	
11	Report writing Chapter1: Introduction; Chapter 2: Literature review and Conceptual framework; Chapter 3: Research Methodology; Chapter 4: …….. Government		May –June 2023															
12	Report writing Chapter 5: ……						J u l y							July –sep 2023				
13	Report writing Chapter 6: Conclusions and Recommendations; Chapter 7: Limitations and Suggestions for further research														Dec -2023			

Sharma